ATTACHMENT B
ITEMS TO BE SEIZED

The items to be seized are fruits, evidence, or instrumentalities of and relating to violations of 18 U.S.C. § 922(n), including:

1. Firearms, firearms paraphernalia, components, accessories, and ammunition;

2. Records and information that constitute evidence of identity, including but not limited to:

   a. Indicia of occupancy and ownership, including bank statements, utilities bills, vehicle registration and vehicle insurance documents.

   b. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, internet search histories, and financial statements—relating to:

      i. Purchase, sale, and/or shipment of firearms, ammunition, and firearms paraphernalia

      ii. Communications and records concerning the sale, shipment, or receipt of firearms and firearm components to individuals prohibited from possessing firearms

      iii. Robertson's knowledge of his criminal charges/prohibited status or his state of mind as it relates to the crime under investigation—excepting any communications protected as a matter of law and privilege—to include the potential punishments, the use of the term "felon" or "felony," internet search histories regarding his case, his charges, or others charged with the same felony offense, and any collateral consequences related to a felony conviction such as a loss of voting rights or inability to possess firearms.

3. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Thomas Robertson about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

4. Computers and/or electronic storage media including all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones,

tablets, servers, and network hardware, such as wireless routers. A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include, but are not limited to, external hard drives, CDs, DVDs and flash drives.

5. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":

a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

e. evidence of the times the Device(s) was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

h. records of or information about Internet Protocol addresses used by the Device(s);

i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search of the Subject Premises, Person, or Vehicle, as described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and

reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device;[1] (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

[1] Law enforcement shall select the finger.